

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020050109685 A
(43)Date of publication of application: 22.11.2005

(21)Application number: 1020040034661
(22)Date of filing: 17.05.2004
(30)Priority: ..

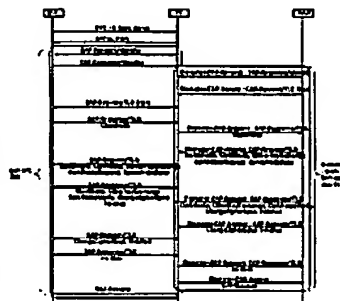
(71)Applicant: SK TELECOM CO., LTD.
(72)Inventor: LEE, DONG KIE
LEE, DONG RYUL
MOON, DONG IL
AHN, JONG GUK

(51)Int. Cl. H04L 9/32

(54) METHOD AND SYSTEM FOR USER AUTHENTICATION BASED ON EAP COEXISTING WITH TERMINAL AUTHENTICATION IN PORTABLE INTERNET SYSTEM, CAPABLE OF UTILIZING CONVENTIONAL PKM AND EAP METHODS WITHOUT MODIFICATION

(57) Abstract:

PURPOSE: A method and a system for user authentication based on an EAP(Extensible Authentication Protocol) coexisting with terminal authentication in a portable internet system are provided to utilize conventional PKM(Privacy Key Management) and EAP methods without modification by performing the user authentication based on the EAP after terminal authentication based on the PKM. **CONSTITUTION:** A mobile subscriber station authentication process is finished by using a PKM protocol. An EAP request transmission message for user authentication is transmitted to a mobile subscriber station. The mobile subscriber station receives the EAP request transmission message for user authentication and transmits an EAP response message. The EAP request transmission message and the EAP response message are exchanged each other and a user authentication result message is transmitted.



copyright KIPO 2006

Legal Status

Date of request for an examination (20050518)
Notification date of refusal decision (00000000)
Final disposal of an application (rejection)
Date of final disposal of an application (20061208)
Patent registration number ()
Date of registration (00000000)
Number of opposition against the grant of a patent ()
Date of opposition against the grant of a patent (00000000)
Number of trial against decision to refuse ()
Date of requesting trial against decision to refuse ()

(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。 Int. Cl.⁷
H04L 9/32

(11) 공개번호 10-2005-0109685
(43) 공개일자 2005년11월22일

(21) 출원번호 10-2004-0034661
(22) 출원일자 2004년05월17일

(71) 출원인 에스케이 텔레콤주식회사
서울 중구 을지로2가 11번지

(72) 발명자 이동기
서울특별시동작구신대방2동709백산아파트101동606호
이동렬
서울특별시성북구상월곡동동아에코빌아파트113동1502호
문동일
강원도원주시명륜2동848-1동보렉스아파트903-802
안중국
서울특별시종로구무악동현대아파트105-1302

(74) 대리인 이철회
송해모

심사청구 : 있음

(54) 휴대 인터넷 시스템에서 단말기 인증과 공존하는 확장된인증 프로토콜 기반의 사용자 인증 방법 및 시스템

요약

본 발명은 휴대 인터넷 시스템에서 단말기 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 방법 및 시스템에 관한 것이다.

본 발명은 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜(EAP : Extensible Authentication Protocol) 기반의 사용자 인증 방법에 있어서, (a) PKM 프로토콜을 이용한 상기 이동 가입자 스테이션 인증이 완료된 후에, 사용자 인증을 위한 EAP 요청 전송 메시지를 상기 이동 가입자 스테이션으로 송신하는 단계; (b) 상기 EAP 요청 전송 메시지를 수신한 상기 이동 가입자 스테이션으로부터 EAP 응답 메시지를 수신하는 단계; 및 (c) 상기 EAP 요청 전송 메시지 및 상기 EAP 응답 메시지가 한 차례 이상 교환된 후에, 사용자 인증 결과 메시지를 송신하는 단계를 포함하는 것을 특징으로 하되, 상기 사용자 인증 방법은 상기 이동 가입자 스테이션 인증과 별개로 수행되는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 방법 및 시스템에 관한 것이다.

본 발명에 의하면, 휴대 인터넷 시스템에서 EAP 기반의 사용자 인증을 PKM(Privacy Key Management) 기반의 단말기 인증 이후에 별개로 수행하게 하여 기존의 PKM 방식과 EAP 방식을 변형 없이 이용할 수 있다는 효과가 있다.

대표도

도 2

작인이

휴대 인터넷 시스템, 단말기 인증, 확장된 인증 프로토콜, 사용자 인증

명세서

도면의 간단한 설명

도 1은 본 발명의 바람직한 실시예에 따른 IIPi 시스템을 개략적으로 나타낸 구성도,

도 2는 본 발명의 바람직한 실시예에 따른 EAP 콜 플로우(Call Flow)를 나타낸 도면이다.

<도면의 주요 부분에 대한 부호의 설명>

100 : 이동 가입자 스테이션 110 : 기지국

120 : ACR 130 : HA

140 : AAA 140 : IP 네트워크

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 휴대 인터넷 시스템에서 단말기 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 방법 및 시스템에 관한 것이다. 더욱 상세하게는, 휴대 인터넷 시스템에서 확장된 인증 프로토콜(Extensible Authentication Protocol : 이하 'EAP'라 함) 기반의 사용자 인증을 PKM(Privacy Key Management) 기반의 단말기 인증 이후에 별개로 수행하게 하여 단말기 인증과 사용자 인증을 가능하게 하고, 특히 AAA(Authentication Authorization Accounting) 서버에 부하가 적은 EAP-MD5(Message Digest)와 같은 방법도 사용할 수 있게 하는 인증 방법 및 시스템에 관한 것이다.

컴퓨터, 전자, 통신 기술이 비약적으로 발전함에 따라 무선 통신망(Wireless Network)을 이용한 다양한 무선 통신 서비스가 제공되고 있다. 가장 기본적인 무선 통신 서비스는 이동 통신 단말기 사용자들에게 무선으로 음성 통화를 제공하는 무선 음성 통화 서비스로서 이는 시간과 장소에 구애받지 않고 서비스를 제공할 수 있다는 특징이 있다. 또한, 문자 메시지 서비스를 제공하여 음성 통화 서비스를 보완해주는 한편, 최근에는 이동 통신 단말기의 사용자에게 무선 통신망을 통해 인터넷 통신 서비스를 제공하는 무선 인터넷 서비스가 대두되었다.

이처럼 이동 통신 기술의 발달로 인해 부호 분할 다중 접속(CDMA : Code Division Multiple Access) 이동 통신 시스템에서 제공하는 서비스는 음성 서비스뿐만이 아니라, 썬킷(Circuit) 데이터, 패킷(Packet) 데이터 등과 같은 데이터를 전송하는 멀티미디어 통신 서비스로 발전해 가고 있다.

또한 최근에는 정보통신의 발달로 ITU-R에서 표준으로 제정하고 있는 제 3 세대 이동 통신 시스템인 IMT-2000(International Mobile Telecommunication 2000)(예컨대, CDMA2000 1X, 3X, EV-DO, WCDMA(WideBand CDMA) 등)이 상용화되고 있다. IMT-2000은 CDMA 2000 1X, 3X, EV-DO, WCDMA(WideBand CDMA) 등으로 기존의 IS-95A, IS-95B 망에서 진화한 IS-95C 망을 이용하여 IS-95A, IS-95B 망에서 지원 가능한 데이터 전송 속도인 14.4 Kbps나 56 Kbps보다 훨씬 빠른 최고 144 Kbps의 전송 속도로 무선 인터넷을 제공할 수 있는 서비스이다. 특히 IMT-2000 서비스를 이용하면 기존의 음성 및 WAP 서비스 품질의 향상은 물론 각종 멀티미디어 서비스(AOD, VOD 등)를 보다 빠른 속도로 제공할 수 있다.

그러나, 기존의 이동 통신 시스템은 기지국 구축 비용이 높기 때문에 무선 인터넷의 이용 요금이 높고, 이동 통신 단말기의 화면 크기가 작기 때문에 이용할 수 있는 콘텐츠에 제약이 있는 등 초고속 무선 인터넷을 제공하기에는 한계가 있다. 또

한, 무선 랜(Wireless Local Area Network) 기술은 전파 간섭 및 좁은 사용 영역(Coverage) 등의 문제로 공중 서비스의 제공에 한계가 있다. 따라서, 휴대성과 이동성이 보장하며 저렴한 요금으로 초고속 무선 인터넷 서비스를 이용할 수 있는 초고속 휴대 인터넷(High-Speed Portable internet; 이하 'HPI'라 칭함) 시스템이 대두되었다.

HPI 시스템은 2.3 GHz 주파수 대역을 사용하며, 듀플렉스(Duplex) 방식으로 TDD(Time Division Duplex), 액세스(Access) 방식으로 OFDMA(Orthogonal Frequency Division Multiple Access)를 사용한다. 또한, 시속 60 km/h의 이동성을 제공하며, 하향 전송 속도는 24.8 Mbps이나 상향 전송 속도는 5.2 Mbps로 상하향 비대칭 전송 특성을 갖는 IP(Internet Protocol) 기반의 무선 데이터 시스템이다.

무선 랜(WLAN : Wireless LAN) 표준인 802.11에서는 여러 가지의 EAP 방법이 채택되어 널리 사용되고 있는데, 이는 WEP(Wired Equivalent Privacy)의 보안 취약성 및 정적 키(Static Key)의 제공 문제에 기인한 것이다. 이러한 이유로 소위 동적(Dynamic) 세션 기반의 WEP이 WLAN에 도입되었다. 동적 세션 기반 WEP의 도입과 함께, WEP 키(Key)들은 EAP-TLS(Transport Layer Security), EAP-TTLS(Tunneled Transport Layer Security), PEAP(Protected Extensible Authentication Protocol) 등을 이용하여 주기적으로 갱신된다. 클라이언트(Client)와 AAA가 마스터 키(Master Key)를 교섭(Negotiation)할 때, 마스터 키는 AAA로부터 AP(Access Point)로 보내진다. 앞서 설명한 바와 같이, EAP은 이러한 WEP의 정적 키 제공 문제 및 보안 취약성에 기인하여 널리 이용되는 것이다.

무선 맨(WMAN : Wireless MAN)은 무선 랜과 다른 인증 방식을 보인다. 최근 제안되고 있는 방식은 기존의 EAP 기법과 PKM 기법을 변형한 방식으로, 우선 EAP를 수행하여 마스터 키를 생성한 후 마스터 키를 PKM에 제공하는 방식이다. 이는 사용자 인증과 단말기 인증이 구분되지 않는 방식이다.

그런데 PKM(Privacy Key Manager)은 잘 정의되어 있는 바, 전술한 WEP의 문제가 발생되지 않는다. EAP-TLS와 같이 클라이언트 측의 인증과 서버 측의 인증을 모두 필요로 하는 공개 키(Public Key) 시스템은 배치(deployment) 및 관리(Management) 문제가 있다. 그러나 이미 존재하고 있는 이동 가입자 스테이션(Mobile Subscriber Station, 이하 'MSS'라 함) 및 기지국(Base Station : 이하 'BS'라 함)은 인증서를 내장하고 있어 배치 및 관리 문제가 발생하지 않는다. 또한 데이터 암호화를 위한 TEK는 주기적으로 갱신되는 바 정적 키 제공 문제가 발생되지 않는다. 그래서 PKM은 WLAN에서 발생하는 보안 문제가 발생되지 않으므로 PKM 수행시 EAP까지 병행하여 수행할 필요는 없다.

또한, EAP-MD5는 마스터 키를 생성하는 메커니즘이 아니므로, 전술한 방식에서는 EAP-MD5를 이용할 수 없다는 문제점이 있다. EAP-MD5는 기본적인 수준의 EAP 지원을 제공하는 EAP 인증 유형의 하나로 AAA에 부하를 줄여줄 수 있는 효율적인 유형인데 이 유형을 이용하지 못한다는 것은 전술한 방식의 약점이 될 수 있다.

또한, 전술한 방법에서처럼 인증 키(Authorization Key)가 EAP AAA 키로부터 나온다면, BS는 다수의 타이머를 관리해야 하는 어려움이 생긴다는 문제점이 있다. 전술한 방법에서 사용되는 타이머를 표로 정리한 것이 표 1이다.

[표 1]

PKM configuration settings	Relation	
Authorize wait timeout		AK
Reauthorize wait timeout		AK
Authorization grace time		AK
Operational wait timeout	TEK	
Rekey wait timeout	TEK	
TEK grace time	TEK	
Authorize reject wait timeout		AK

표 1에서 보이는 바와 같이, 7개의 타이머가 Auth Reply 메시지와 함께 전달된다. 전송한 방식과 같이 EAP 와 PKM이 혼용되어 사용되면 이러한 타이머 중 4개는 AAA로부터 전송되고, BS는 EAP 메시지를 해석하고, TEK 관련 타이머 값을 해석하고 이러한 7개의 타이머를 조합하여 MSS로 전달해야 한다. 이는 BS에게 다수의 타이머를 관리해야 하는 어려움을 야기하게 된다는 문제점이 있다.

발명이 이루고자 하는 기술적 과제

전술한 문제점을 해결하기 위해 본 발명은, 휴대 인터넷 시스템에서 EAP 기반의 사용자 인증을 PKM(Privacy Key Management) 기반의 단말기 인증 이후에 별개로 수행하게 하여 단말기 인증과 사용자 인증을 가능하게 하고, 특히 AAA(Authentication Authorization Accounting) 서비스에 부하가 적은 EAP-MD5(Message Digest)와 같은 방법도 사용할 수 있게 하는 인증 방법 및 시스템을 제공하는 것을 목적으로 한다.

발명의 구성 및 작용

본 발명의 제 1 목적에 의하면, 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜(EAP : Extensible Authentication Protocol) 기반의 사용자 인증 방법에 있어서, (a) PKM 프로토콜을 이용한 상기 이동 가입자 스테이션 인증이 완료된 후에, 사용자 인증을 위한 EAP 요청 전송 메시지를 상기 이동 가입자 스테이션으로 송신하는 단계; (b) 상기 EAP 요청 전송 메시지를 수신한 상기 이동 가입자 스테이션으로부터 EAP 응답 메시지를 수신하는 단계; 및 (c) 상기 EAP 요청 전송 메시지 및 상기 EAP 응답 메시지가 한 차례 이상 교환된 후에, 사용자 인증 결과 메시지를 송신하는 단계를 포함하는 것을 특징으로 하되, 상기 사용자 인증 방법은 상기 이동 가입자 스테이션 인증과 별개로 수행되는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 방법을 제공한다.

본 발명의 제 2 목적에 의하면, 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜(EAP : Extensible Authentication Protocol) 기반의 사용자 인증 시스템에 있어서, EAP 요청 전송 메시지인 EAP-REQ 메시지를 수신하면 그에 응답하여 EAP 응답 메시지인 EAP-RSP 메시지를 전송하는 이동 가입자 스테이션; 및 PKM 프로토콜을 이용한 상기 이동 가입자 스테이션 인증이 완료된 후에, 사용자 인증을 위한 EAP 요청 전송 메시지를 상기 이동 가입자 스테이션으로 송신하고 상기 이동 가입자 스테이션으로부터 EAP 응답 메시지를 수신하여, 상기 EAP 요청 전송 메시지 및 상기 EAP 응답 메시지가 한 차례 이상 교환된 후에 상기 이동 가입자 스테이션으로 사용자 인증 결과 메시지를 송신하는 기지국을 포함하는 것을 특징으로 하되, 상기 사용자 인증은 상기 이동 가입자 스테이션 인증과 별개로 수행되는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 시스템을 제공한다.

이하, 본 발명의 바람직한 실시예를 첨부된 도면들을 참조하여 상세히 설명한다. 우선 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

도 1은 본 발명의 바람직한 실시예에 따른 HPI 시스템을 개략적으로 나타낸 구성도이다.

도 1에 도시한 바와 같이, HPI 시스템은 MSS(Mobile Subscriber Station)(100), AP(Access Point)인 기지국(BS : Base Station)(110), 여러 개의 기지국(110)을 수용하는 액세스 컨트롤 라우터인 ACR(Access Control Router)(120), HIA(Home Agent)(130), AAA(Authentication, Authorization, Accounting)(140), IP 네트워크(140) 및 인터넷(160) 등을 포함할 수 있다.

여기서, 본 발명의 바람직한 실시예에 따른 MSS(100)는 HPI 시스템에 접속하여 초고속 무선 인터넷 서비스를 이용하는 이동 통신 단말기를 말하며, 저전력 RF(Radio Frequency)/IF(Intermediate Frequency) 모듈 및 컨트롤러 기능, 서비스 특성 및 전파 환경에 따른 MAC(Media Access Control) 프레임 가변 제어 기능, 핸드오프 기능, 인증 및 암호화 기능 등을 수행한다.

본 발명의 바람직한 실시예에 따른 MSS(100)는 BS(110)로부터 EAP 요청 전송 메시지인 EAP-REQ 메시지를 수신하면 그에 응답하여 EAP 응답 메시지인 EAP-RSP 메시지를 전송하여 EAP를 이용한 사용자 인증을 가능하게 한다.

본 발명의 바람직한 실시예에 따른 기지국(110)은 HPI 시스템의 AP로서 ACR(120)로부터 수신한 데이터를 무선으로 MSS(100)에 전송하게 되며, 저전력 RF/IF 모듈 및 콘트롤러 기능, OFDMA/TDD 패킷 스케줄링과 채널 다중화 기능, 서비스 특성 및 전파 환경에 따른 MAC 프레임 가변 제어 기능, 50 Mbps급 고속 트래픽 실시간 제어 기능, 핸드오프 기능 등을 갖는다.

본 발명의 바람직한 실시예에 따른 기지국(110)은 사용자 인증을 위해 EAP 요청 전송 메시지(Request Transfer Message)를 MSS(100)에 전송함으로써 사용자 인증을 시작한다. 수 개의 EAP 요청 전송 메시지가 교환된 후에, EAP 성공(Success) 또는 실패(Failure) 메시지가 BS(110)로부터 MSS(100)로 보내진다. 만약 사용자 인증이 실패하면 BS(110)는 해당 MSS(100)와 관계된 모든 세션 정보를 종결시키거나 세션 정보를 그대로 유지한다. EAP 프로토콜 및 이를 이용한 사용자 인증에 대한 자세한 내용은 후술하기로 한다.

한편, 본 발명의 바람직한 실시예에 따른 MSS(100) 및 기지국(110)은 데이터 전송을 위한 50 Mbps 패킷 전송 변복조 기능, 고속 패킷 채널 코딩 기능, 실시간 모뎀 제어 기능 등을 갖는다.

본 발명의 바람직한 실시예에 따른 ACR(120)은 다수 개의 기지국(110)을 수용하는 액세스 콘트롤 라우터로서 기지국(110)간의 핸드오프 제어 기능, ACR(120)간의 핸드오프 기능, 패킷 라우팅 기능, 인터넷 접속 기능 등을 가지며, IP 네트워크(150)에 접속된다.

본 발명의 바람직한 실시예에 따른 HA(130)는 인터넷(160) 등의 외부 패킷 데이터 서비스 서버로부터 패킷을 전송하는 라우팅(Routing)을 수행하며, AAA(140)는 기지국(110)과 연동하여 MSS(100)에서 이용한 패킷 데이터에 대한 과금을 수행하고, MSS(100)로부터의 접속을 인증한다.

본 발명의 바람직한 실시예에 따른 IP 네트워크(150)는 기지국(110), ACR(120), HA(130) 및 AAA(140) 등을 연결시켜 주고, 인터넷(160) 등의 외부 패킷 데이터 서비스로부터 패킷 데이터를 전달받아 기지국(110)에 전송한다.

본 발명의 바람직한 실시예는 단말기 인증인 PKM 인증과 사용자 인증인 EAP가 별개로 수행되는 것을 특징으로 한다. 본 발명의 바람직한 실시예에 따른 EAP 방식은 PKM 키 교환이 완료된 이후에 수행된다. 만약 세컨더리 매니지먼트(Secondary Management) CID가 이용되면, EAP 교환은 PKM과 교섭된 데이터 암호화 방식을 이용하여 보호된다. 그러나 만약 EAP 교환이 EAP-TLS(Transport Layer Security) 또는 EAP-TTLS(Tunneled Transport Layer Security)와 같이 암호화를 필요로 하지 않는다면 프라이머리 매니지먼트(Primary Management) CID가 이용되는 바, PKM과는 아무런 관계가 없게 된다.

도 2는 본 발명의 바람직한 실시예에 따른 EAP 콜 플로우(Call Flow)를 나타낸 도면이다.

도 2에 도시된 바와 같이, EAP 요청 메시지(Request Transfer Message)는 BS(110)로부터 MSS(100)로 보내진다. 그러나 PKM 요청 전송 메시지는 MSS(100)로부터 BS(110)로 보내지므로 EAP 요청 전송 메시지는 PKM 요청 전송 메시지에 매핑되지 않는다.

도 2에 도시된, MAC 매니지먼트 메시지를 표로 나타낸 것이 표 2이다.

[표 2]

Type	Message	Message Description	Connection
60	MOB-HO-IND	HO indication message	basic
63	EAP-REQ	EAP Request Transfer message	primary
64	EAP-RSP	EAP Response Transfer message	primary
65-255	reserved		

도 2에 도시된 EAP-REQ 메시지는 EAP 요청 전송 메시지로써, BS(110)가 암호화된 EAP 요청 인증 데이터를 나르도록 하기 위해 보내진다. EAP-REQ 메시지의 포맷을 나타낸 것이 표 3이다.

[표 3]

Syntax	Size	Notes
<u>EAP-REQ Message Format()</u> {		
<u>Management Message Type = 63</u>	<u>8 bits</u>	
<u>Transaction ID</u>	<u>16 bits</u>	
<u>TLV Encoded Information</u>	<u>Variable</u>	<u>TLV specific</u>
}		

EAP-REQ 메시지는 CID, MSS(100)의 프라이머리 매니지먼트 CID 및 트랜잭션(Transaction) ID 등의 파라미터를 포함한다. 여기서 트랜잭션 ID는 센터(Sender)에 의해 할당되는 트랜잭션의 고유 식별자이다. 또한, 이러한 모든 파라미터는 TLV 집합으로서 코딩된다. 여기서 TLV 집합은 SAID(Security Association ID), EAP Payload 및 HMAC Tuple 등이 될 수 있다. 여기서, HMAC Tuple 어트리뷰트는 센터를 인증하기 위한 메시지 다이제스트를 포함하며, EAP 메시지의 어트리뷰트 리스트 내에 최종 어트리뷰트가 된다.

한편, 도 2에 도시된 EAP-RSP 메시지는 수신된 EAP-REQ 메시지에 대한 응답으로서 생성되며, EAP 응답을 포함한다. MSS(100)가 EAP-REQ 메시지를 받고 EAP-RSP 메시지를 전송하지 않으면, BS(110)는 EAP Payload 없이 EAP-RSP 메시지를 전송한다. EAP-RSP 메시지의 포맷을 나타낸 것이 표 4이다.

[표 4]

Syntax	Size	Notes
<u>EAP-REQ Message Format()</u> {		
<u>Management Message Type = 64</u>	<u>8 bits</u>	
<u>Transaction ID</u>	<u>16 bits</u>	
<u>TLV Encoded Information</u>	<u>Variable</u>	<u>TLV specific</u>
}		

EAP-RSP 메시지는 CID, MSS(100)의 프라이머리 매니지먼트 CID 및 대응되는 EAP-REQ 메시지로부터의 트랜잭션(Transaction) ID 등의 파라미터를 포함한다. 또한, 이러한 모든 파라미터는 TLV 집합으로서 코딩된다. 여기서 TLV 집합은 SAID(Security Association ID), EAP Payload 및 HMAC Tuple 등이 될 수 있다. 여기서, HMAC Tuple 어트리뷰트는 센터를 인증하기 위한 메시지 다이제스트를 포함하며, EAP 메시지의 어트리뷰트 리스트 내에 최종 어트리뷰트가 된다.

본 발명의 바람직한 실시예에 따른 인증 프로토콜은 암호화(Encapsulation) 프로토콜, PKM(Privacy Key Management) 프로토콜 및 EAP 프로토콜 등이 있다.

우선, 암호화 프로토콜은 고정된 광대역 무선 접속(BWA : Broadband Wireless Access) 네트워크를 지나온 패킷 데이터의 보안을 위한 것이다. 이 프로토콜은 데이터 암호화 편성 및 인증 알고리즘과 같은 Cryptographic Suites의 집합 및 MAC PDU 페이로드에 대한 알고리즘을 적용하기 위한 규칙 등을 정의한다.

한편, PKM 프로토콜은 BS(110)로부터 MSS(100)로 키(Key)를 가진 데이터의 안전한 분배를 제공한다. 이러한 PKM 프로토콜을 통해 MSS(100)와 BS(110)는 키를 가진 데이터를 동기화하고, BS(110)는 네트워크 서비스에 대한 액세스를 강화하는 데 이 프로토콜을 이용한다. PKM 프로토콜을 이용하여 MSS(100)를 인증하고 인증키를 교환하게 된다.

또한, EAP 프로토콜은 EAP를 사용하여 사용자 인증을 제공한다. EAP 방식에 기반한 사용자 인증을 통해 BS(110)는 MSS(100)를 인증하고, MSS(100)는 BS(110)를 인증한다.

PKM 프로토콜을 이용하여 MSS(100) 인증과 인증키 교환이 완료된 후에 BS(110)는 EAP 요청 전송 메시지(Request Transfer Message)를 MSS(100)에 전송함으로써 사용자 인증을 시작한다. 수 개의 EAP 요청 전송 메시지가 교환된 후에, EAP 성공(Success) 또는 실패(Failure) 메시지가 BS(110)로부터 MSS(100)로 보내진다. 만약 사용자 인증이 실패하면 BS(110)는 해당 MSS(100)와 관계된 모든 세션 정보를 종결시키거나 세션 정보를 그대로 유지한다. 이처럼, EAP 방식은 오퍼레이터(Operator)의 필요 요청에 따라 이용된다.

이처럼 본 발명의 바람직한 실시예에 따르면, EAP를 이용한 사용자 인증과 PKM을 이용하는 단말기 인증이 분리되어 수행되게 된다. 즉, EAP 키 교환 및 사용자 인증이 PKM을 이용하는 단말기 인증이 완료된 후에 수행되는 것이다. 따라서, 종래 방법과는 달리, 인증키(AK) 스테이트 머신은 AAA(140)에 의해 관리되고, 단말기 암호화 키(TEK) 스테이트 머신은 BS(110)에 의해 관리되므로, 타이머 값이 BS(110)와 AAA(140) 사이에서 분리되어 정의된다는 특징이 있다.

한편, 본 발명의 바람직한 실시예에 따른 EAP를 이용한 사용자 인증 유형으로는 EAP-MD-5, EAP-TLS, EAP-PEAP, EAP-TTLS, LEAP 및 PEAP가 있다.

EAP-MD-5(Message Digest)는 기본적인 수준의 EAP 지원을 제공하는 EAP 인증 유형이다. EAP-MD-5는 사용자 암호를 알아낼 수 있으므로 일반적으로 무선 LAN 구현에는 권장되지 않는다. 이 인증 유형은 실제로는 무선 클라이언트와 네트워크에 대한 상호 인증 단계가 없으므로 단방향 인증만 제공한다. 또한 동적인 세션 기반 WEP 키를 알아낼 수 있는 방법을 제공하지 않는다는 점에서 매우 중요한 인증 유형 중 하나이다.

EAP-TLS(Transport Layer Security)는 클라이언트 및 네트워크에 대한 인증서 기반 상호 인증 기능을 제공한다. 이 방법은 클라이언트측 인증서와 서버측 인증서를 통해 인증을 수행하며 WLAN 클라이언트와 액세스 포인트 간 후속 통신에 대한 보안을 강화하기 위해 사용자 기본 WEP 키 및 세션 기반 WEP 키를 동적으로 생성한다. EAP-TLS의 한 가지 단점은 클라이언트측과 서버측 모두에서 인증서를 관리해야 한다는 점이다.

EAP-TTLS(Tunneled Transport Layer Security)는 암호화된 채널(또는 "터널")을 통해 클라이언트와 네트워크에 대한 인증서 기반 상호 인증 및 동적인 사용자 또는 세션 기반 WEP 키를 생성할 수 있는 방법을 제공한다. EAP-TLS와 달리 EAP-TTLS에는 서버측 인증서만 있으면 된다.

LEAP(Lightweight Extensible Authentication Protocol)는 주로 Cisco Aironet WLAN에서 사용하는 EAP 인증 유형으로, 동적으로 생성된 WEP 키를 사용하여 전송 데이터를 암호화하며 상호 인증을 지원한다.

PEAP(Protected Extensible Authentication Protocol)는 레거시 암호 기반 프로토콜과 같은 인증 데이터를 802.11 무선 네트워크를 통해 안전하게 전송할 수 있는 방법을 제공한다. PEAP는 PEAP 클라이언트와 인증 서버 간 터널링을 사용하여 이 기능을 수행한다. PEAP는 유사한 기능을 수행하는 TTLS(Tunneled Transport Layer Security)와 같이 서버측 인증서만을 사용하여 보안 무선 LAN의 구현 및 관리를 간소화함으로써 무선 LAN 클라이언트를 인증한다.

이처럼 본 발명의 바람직한 실시예에 따르면, EAP를 이용한 사용자 인증과 PKM을 이용하는 단말기 인증이 분리되어 수행되므로 종래 방법에서 이용하지 못했던 EAP-MD5도 이용할 수 있게 됨에 따라 AAA(140)에 대한 오버헤드도 상당 부분 낮출 수 있게 되었다.

이상의 설명은 본 발명을 예시적으로 설명한 것에 불과한 것으로, 본 발명이 속하는 기술분야에서 통상의 지식을 가지는 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 변형이 가능할 것이다. 따라서, 본 명세서에 개시된 실시예들은 본 발명을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 사상과 범위가 한정되는 것은 아니다. 본 발명의 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

발명의 효과

이상 설명한 바와 같이 본 발명에 의하면, 휴대 인터넷 시스템에서 EAP 기반의 사용자 인증을 PKM(Privacy Key Management) 기반의 단말기 인증 이후에 별개로 수행하게 하여 기존의 PKM 방식과 EAP 방식을 변형 없이 이용할 수

다는 효과가 있다. 또한, 종래 이용하지 못했던 EAP-MD5(Message Digest)와 같은 방식도 이용할 수 있게 함으로써 모든 EAP 방식을 사용할 수 있게 되어 적용 유연성을 가지게 되고, 이러한 EAP-MD5는 AAA에 부하가 적은 방식이므로 더 효율적으로 사용자 인증을 가능하게 한다는 장점이 있다.

(57) 청구의 범위

청구항 1.

휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜(EAP : Extensible Authentication Protocol) 기반의 사용자 인증 방법에 있어서,

(a) PKM 프로토콜을 이용한 상기 이동 가입자 스테이션 인증이 완료된 후에, 사용자 인증을 위한 EAP 요청 전송 메시지를 상기 이동 가입자 스테이션으로 송신하는 단계;

(b) 상기 EAP 요청 전송 메시지를 수신한 상기 이동 가입자 스테이션으로부터 EAP 응답 메시지를 수신하는 단계; 및

(c) 상기 EAP 요청 전송 메시지 및 상기 EAP 응답 메시지가 한 차례 이상 교환된 후에, 사용자 인증 결과 메시지를 송신하는 단계

를 포함하는 것을 특징으로 하되, 상기 사용자 인증 방법은 상기 이동 가입자 스테이션 인증과 별개로 수행되는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 방법.

청구항 2.

제 1 항에 있어서,

상기 EAP 기반의 사용자 인증은 EAP-MD5, EAP-TLS, EAP-TTLS, LEAP 및 PEAP 중 하나 이상을 포함하는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 방법.

청구항 3.

제 1 항에 있어서,

상기 사용자 인증이 실패하면, 기지국은 상기 이동 가입자 스테이션과 관계된 모든 세션을 종결시키는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 방법.

청구항 4.

제 1 항에 의하면,

상기 사용자 인증이 실패하면, 기지국은 상기 이동 가입자 스테이션과 관계된 현재 세션 정보를 유지하는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 방법.

청구항 5.

제 1 항에 있어서,

상기 EAP 요청 전송 메시지 및 상기 EAP 응답 메시지는 CID, 상기 이동 가입자 스테이션의 프라이머리 매니지먼트 CID 및 트랜잭션 ID 정보를 파라미터로 포함하는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 방법.

청구항 6.

제 5 항에 있어서,

상기 파라미터는 TLV 집합으로서 코딩되는데, 상기 TLV 집합은 SAID(Security Association ID), EAP Payload 및 HMAC Tuple을 포함하는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 방법.

청구항 7.

휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜(EAP : Extensible Authentication Protocol) 기반의 사용자 인증 시스템에 있어서,

EAP 요청 전송 메시지인 EAP-REQ 메시지를 수신하면 그에 응답하여 EAP 응답 메시지인 EAP-RSP 메시지를 전송하는 이동 가입자 스테이션; 및

PKM 프로토콜을 이용한 상기 이동 가입자 스테이션 인증이 완료된 후에, 사용자 인증을 위한 EAP 요청 전송 메시지인 상기 이동 가입자 스테이션으로 송신하고 상기 이동 가입자 스테이션으로부터 EAP 응답 메시지를 수신하여, 상기 EAP 요청 전송 메시지 및 상기 EAP 응답 메시지가 한 차례 이상 교환된 후에 상기 이동 가입자 스테이션으로 사용자 인증 결과 메시지를 송신하는 기지국

을 포함하는 것을 특징으로 하되, 상기 사용자 인증은 상기 이동 가입자 스테이션 인증과 별개로 수행되는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 시스템.

청구항 8.

제 7 항에 있어서,

상기 EAP 기반의 사용자 인증은 EAP-MD5, EAP-TLS, EAP-TTLS, LEAP 및 PEAP 중 하나 이상을 포함하는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 시스템.

청구항 9.

제 7 항에 있어서,

상기 사용자 인증이 실패하면, 상기 기지국은 상기 이동 가입자 스테이션과 관계된 모든 세션을 종결시키는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 시스템.

청구항 10.

제 7 항에 의하면,

상기 사용자 인증이 실패하면, 상기 기지국은 상기 이동 가입자 스테이션과 관계된 현재 세션 정보를 유지하는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 시스템.

청구항 11.

제 7 항에 있어서,

상기 EAP 요청 전송 메시지 및 상기 EAP 응답 메시지는 CID, 상기 이동 가입자 스테이션의 프라이머리 매니지먼트 CID 및 트랜잭션 ID 정보를 파라미터로 포함하는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 시스템.

청구항 12.

제 11 항에 있어서,

상기 파라미터는 TLV 집합으로서 코딩되는데, 상기 TLV 집합은 SAID(Security Association ID), EAP Payload 및 HMAC Tuple을 포함하는 것을 특징으로 하는 휴대 인터넷 시스템에서 이동 가입자 스테이션 인증과 공존하는 확장된 인증 프로토콜 기반의 사용자 인증 시스템.

도면

도면1

